3. NtSetTimerResolution : информ. портал. URL: http://undocumented.ntinternals.net/UserMode/Undocumented%20Functions/Time/NtSetTimerResolution.html (дата обращения: 05.11.2013).

4. timeBeginPeriod function : информ. портал. URL: http://msdn.microsoft.com/en-us/library/windows/desktop/dd757624(v=vs.85).aspx (дата обращения: 05.11.2013).

5. Windows Sysinternals : информ. портал. URL: http://technet.microsoft.com/ru-ru/sysinternals/bb897568.aspx (дата обращения: 07.11.2013).

МЕТОД ЗАЩИТЫ ОТ ПЕРЕХВАТА ПАКЕТОВ АВТОРИЗАЦИИ ПРИ БЕСПРОВОДНОЙ ПЕРЕДАЧЕ ДАННЫХ

Д. О. Деденев, М. П. Трухин
(Екатеринбург, УрФУ, danes1@mail.ru)

Постановка задачи

В данной работе рассматривается принцип взаимодействия между пользователем и беспроводной точкой доступа, т. е. то, каким образом осуществляется процесс подключения к точке доступа, как и при каких условиях передается ключ аутентификации, возможно ли влияние посторонним оборудованием на канал связи между авторизированным устройством и точкой доступа.

Процедура поиска уязвимости

Воспользуемся операционной средой Black Track 5 R1, с помощью которой мы сможем пронаблюдать за поведением устройств, отсылающих запросы подключения.

Переведем наше беспроводное оборудование в режим прослушивания эфира, в результате чего сможем наблюдать обнаруженные точки доступа.

В следующем окне увидим, например, что у нас получилось найти 3 беспроводных точки доступа со следующим наименованием и их MAC-адресами (рис.1):

– Tarasun MAC = 00:25:86:25:9B:2C
– sv-home MAC = 00:15:6D:EE:EA:F6
– Allysia MAC = 54:E6:FC:BA:35:1C

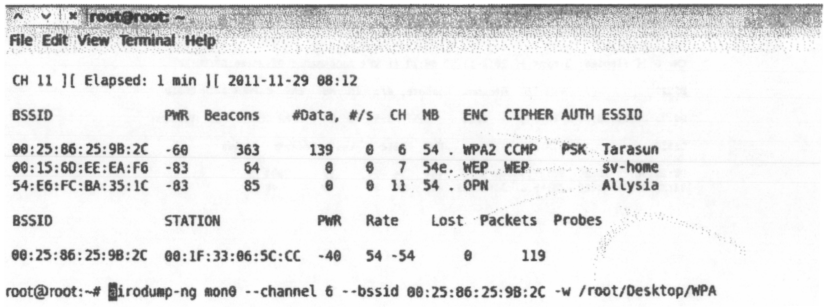

Рис. 1. Содержимое окна с атрибутами точек доступа

В приведенном примере также видно, что к одной из точек доступа (к Tarasun) подключено какое-то устройство с MAC-адресом 00:1F:33:06:5C:CC.

За одну минуту прослушивания канала было передано 119 пакетов. Это может говорить о том, что есть постоянная связь между оборудованием и пользователем. Но за то время, пока мы просматривали эфир, передачи пакета с захешированным ключом не состоялось.

Среди функций данной программы есть способ осуществить разрыв связи между адресом 00:25:86:25:9b:2c и адресом 00:1F:33:06:5C:CC. Для этого с нашей стороны прописывается функция

root@bt:~# aireplay-ng --deauth 5 00:25:86:25:9b:2c 00:1F:33:06:5C:CC wlan1,

где (рис. 2)

– --deauth 5 – отправление 5 запросов на разрыв связи;

– 00:25:86:25:9b:2c – MAC-адрес точки доступа;

– 00:1F:33:06:5C:CC – MAC подключенного оборудования к точке доступа:

– wlan1 – наше устройство, с помощью которого мы прослушиваем канал связи.

После вызова данной функции произошел разрыв между адресами Tarasun и 00:1F:33:06:5C:CC, в результате чего за последующие 2 мин. было передано 9904 пакета. Данная программа умеет определять, был передан пароль или нет. Поскольку в данном при-

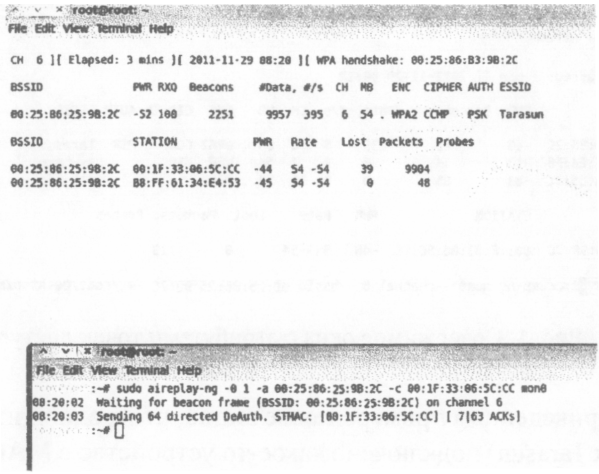

Рис. 2. Содержимое окна с откликом
на функцию root@bt:~# aireplay-ng

мере мы осуществили разрыв, то оборудованию пользователя необходимо было передать зашифрованный пароль, и программа это обнаружила. На верхней части рис. 2, в первой строчке (в ее конце) написано:

WPA hadshake : 00:25:86:25:9b:2c,

т. е. мы заполучили зашифрованный пароль. В дальнейшем, используя высокопроизводительное оборудование, можно расшифровать этот пароль.

Выводы

В результате проведения этого небольшого исследования можно убедиться в том, что постороннее оборудование способно влиять на каналы связи между подключенным оборудованием и точкой доступа. Самое нежелательное, что может при этом произойти, – это получение пакетов, передающихся с устройства, совершающего подключение к точке доступа с зашифрованным паролем, который в дальнейшем может быть расшифрован и, тем самым, посторонний пользователь может получить доступ к зашифрованной информации, содержащейся в остальных пакетах.